(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 197 11 478 A 1**

(51) Int. Cl.[6]:
G 06 F 12/14
G 06 F 11/00
G 06 K 19/07

(21) Aktenzeichen: 197 11 478.4
(22) Anmeldetag: 19. 3. 97
(43) Offenlegungstag: 1. 10. 98

(71) Anmelder:
Siemens AG, 80333 München, DE

(72) Erfinder:
Nolles, Jürgen, 81825 München, DE; Viehmann, Hans-Heinrich, 81739 München, DE

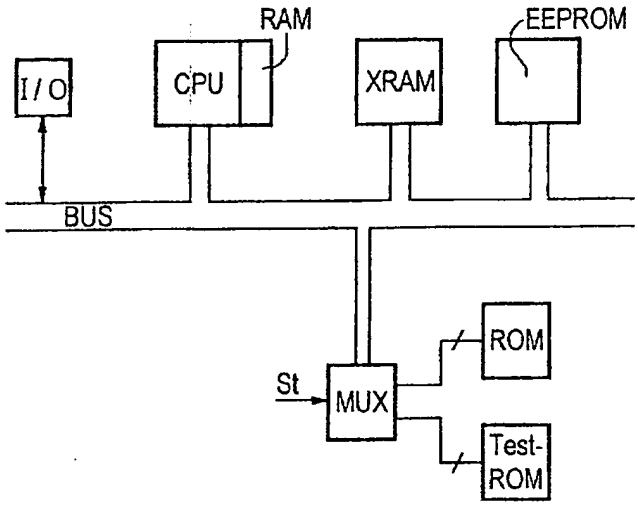
(56) Entgegenhaltungen:
DE 38 33 938 C2

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Integrierte Schaltung und Verfahren zum Testen der integrierten Schaltung

(57) Integrierte Schaltung mit einer CPU und einem Anwender-ROM, gekennzeichnet durch ein Test-ROM, dessen Adreßraum innerhalb des Anwender-ROM-Adreßraums liegt, ein CPU externes RAM sowie ein Schaltmittel, das einen Zugriff nur entweder auf das Anwender-ROM oder das Test-ROM ermöglicht und irreversibel in einen Zustand versetzbar ist, der nur einen Zugriff auf das Anwender-ROM erlaubt.



DE 197 11 478 A 1

DE 197 11 478 A 1

Beschreibung

Die ersten Chipkartengenerationen wie Telefonkarten oder Krankenhauskarten konnten im wesentlichen nur Speicherfunktionen ausführen. Später kamen verhältnismäßig einfache Logikfunktionen wie Zahlenvergleich oder Erzeugen von Pseudozufallszahlen hinzu. Mit dem zunehmenden Einsatz von Chipkarten in sicherheitsrelevanten Bereichen wie im Bankgewerbe, wo teils erhebliche Werte gespeichert werden oder wenn besonders vertrauliche Daten gespeichert sind, kommt zunehmend ein Mikroprozessor zum Einsatz, der die komplexen Sicherungs-, Verschlüsselungs- und/oder Authentifizierungsoperationen ausführen kann. In zunehmendem Maße kommen auch kryptologische Verfahren zum Einsatz, die einen erheblichen Rechenaufwand erfordern.

Die in heutigen Chipkarten enthaltenen Halbleiterchips beinhalten also aufwendige und komplexe Schaltungen, die in der Regel mit einer CPU, einem ROM, einem EEPROM (oder EPROM) sowie teilweise weiteren Modulen wie einem UART, oder einem Koprozessor und einem diese verbindenden Bus gebildet sind. Der CPU ist zumeist ein RAM, das meistens als statisches RAM ausgeführt ist, zugeordnet. Da statische RAMs einen erheblichen Platzbedarf haben, sind sie meist sehr klein und weisen nur weniger als ein KByte Speicherkapazität auf. Charakteristisch für Chipkartenprodukte ist außerdem, daß sie nur ein bis zwei serielle Schnittstellen zur Außenwelt haben, wodurch eine Datenübertragung sehr langsam erfolgt. Da intern eine parallele Verarbeitung mit 8 Bit erfolgt, ist eine Serien/Parallel-Wandlung nötig, die mittels des Akkumulators per CPU softwaregesteuert erfolgt, wodurch auch diese Wandlung sehr langsam abläuft. Da die normale Datenübertragung aber durch eine ISO-Norm definiert ist und nur mit einigen KBit pro Sekunde erfolgt, stellt dies für den Normalbetrieb, also den Betrieb beim Anwender zum bestimmungsgemäßen Gebrauch als beispielsweise wiederaufladbare Geldbörse, kein Problem dar.

Die beschriebenen komplexen integrierten Schaltungen müssen jedoch in ausreichender Qualität an die Kunden ausgeliefert werden, so daß umfangreiche Tests notwendig sind.

Diese Produkttests werden mit Hilfe einer Selftest-Software durchgeführt. Deshalb beinhalten Chipkartenprodukte einen Testspeicher, der als ROM ausgeführt ist. Dieser enthält die Selftest-Software, mit deren Hilfe nach einem Power-on Reset Teile des Chips getestet werden können. Die Selftest-Software besteht aus verschiedenen Testroutinen, die über Testvektoren aufgerufen werden. Diese Testvektoren können über den IO-Port eingegeben werden. Da die Größe des Testspeichers begrenzt ist und innerhalb der verschiedenen Produkte schwankt, enthält er in der Regel nicht alle Testroutinen. Deshalb müssen die übrigen Testroutinen in das EEPROM nachgeladen werden und von dort ausgeführt werden. Hierfür sind mehrere Programmier- und Löschvorgänge nötig, die im Vergleich zum eigentlichen Test wesentlich länger dauern.

Der als ROM ausgeführte Testspeicher ist Bestandteil des auf dem Halbleiter-Chip vorhandenen ROMs, das auch Anwenderprogramme wie das Betriebssystem und häufig verwendete Unterprogramme wie EEPROM-Schreib- und Löschprogramme enthält. Der Testspeicherbereich nimmt also einen Teil des Adressraums des ROMs in Anspruch, so daß ein irrtümlicher oder auch absichtlicher und mißbräuchlicher Einsprung in diesen Adressbereich möglich ist, selbst wenn durch bestimmte Maßnahmen ein Zugriff auf diesen Adressbereich des ROMs nach den durchgeführten Tests zu unterbinden versucht wird.

Die bisherige Realisierung hat also den Nachteil einerseits zu langsam zu sein, so daß die Tests zu lange dauern und damit teuer sind und andererseits auch nach dem Test einen Zugriff auf die Testroutinen zu ermöglichen, da diese in einem ROM quasi fest verdrahtet sind oder in einem EEPROM möglicherweise nicht-flüchtig auf dem Chip verbleiben können.

Die Aufgabe vorliegender Erfindung ist es also, eine Schaltungsanordnung anzugeben, die einen schnellen Test erlaubt und einen hohen Schutz vor Mißbrauch bietet.

Die Aufgabe wird durch eine integrierte Schaltung gelöst, die zumindest eine CPU, ein Anwender-ROM, ein Test-ROM und eine CPU-internes RAM umfaßt. Der Adreßraum des Test-ROMs liegt dabei innerhalb des Adreßraums des Anwender-ROMs, wobei in erfindungsgemäßer Weise ein Schaltmittel vorgesehen ist, das einen Zugriff nur entweder auf das Anwender-ROM oder das Test-ROM ermöglicht. In vorteilhafter Weiterbildung ist das Schaltmittel irreversibel in einen Zustand versetzbar, der nur einen Zugriff auf das Anwender-ROM erlaubt. Auf diese Weise kann nach Abschluß der Testphase das Test-ROM gesperrt werden, ohne daß dessen früherer Adreßraum nicht mehr belegt ist. Es ist somit keine Lücke im zur Verfügung stehenden Adreßbereich vorhanden, in dem gesperrte Speicherbereiche liegen können, so daß ein Angreifer hieraus keinen Nutzen ziehen kann.

In Weiterbildung der Erfindung steht im Test-ROM lediglich ein zum Starten eines Tests unbedingt erforderliches Testbeginnprogramm. Damit werden die eigentlichen Testroutinen in ein CPU-externes, also zusätzliches RAM, ein sogenanntes X-RAM geschrieben, von wo sie dann ausgeführt werden.

Ein erfindungsgemäßes Verfahren ist in Anspruch 7 angegeben. Eine Speicherung der Testroutine lediglich in einem X-RAM hat den Vorteil, daß nach einem Test durch Abschalten der Versorgungsspannung die Testroutinen gelöscht werden können, da das X-RAM flüchtig ist.

Bei Chipkartenanwendungen steht normalerweise nur ein serielles Eingangs/Ausgangstor zur Verfügung, da dort nur eine begrenzte Anzahl von Kontakten zur Kommunikation mit der Außenwelt vorgesehen ist. Die Serien/Parallel- bzw. Parallel/Serien-Wandlung übernimmt der von der CPU gesteuerte Akkumulator. Dies erfolgt softwaregesteuert und ist entsprechend langsam. In Weiterbildung der Erfindung ist deshalb ein aktivier- und deaktivierbares Schieberegister vorhanden, das das Eingangs/Ausgangstor zusätzlich mit einem internen Bus verbindet. Damit können die Testroutinen wesentlich schneller in das X-RAM geschrieben werden.

In weiterer Ausbildung der Erfindung kann dieses Schieberegister dazu benutzt werden, während eines Test auftretende Signale zur Überwachung nach außen in das Testgerät zu überführen. Damit kann der Test sicherer und schneller gemacht werden. Es ist dabei vorteilhaft, diese Signale vor der Übertragung zu verschlüsseln, was in vorteilhafter Weise durch eine lineare oder nicht-lineare Rückkopplung des Schieberegisters, beispielsweise durch ein XOR-Gatter, geschehen kann. Es sind aber auch andere Gatterfunktionen möglich.

Die Erfindung wird nachfolgend anhand eines Ausführungsbeispiels mit Hilfe von **Fig.** näher beschrieben. Dabei zeigen:

Fig. 1 ein Blockschaltbild einer erfindungsgemäßen integrierten Schaltung und

Fig. 2 ein detaillierteres Schaltbild einer vorteilhaften Ausführung der Erfindung.

Gemäß **Fig.** 1 sind eine CPU samt ihr zugeordnetem RAM, ein zusätzliches X-RAM sowie ein nicht-flüchtiges EEPROM über einen Bus miteinander verbunden. Ein serielles Eingangs/ Ausgangstor I/O ist mit dem in der CPU ent-

haltenen (nicht dargestellten) Akkumulator, der auch zur Serien/Parallel-Wandlung dient über den Bus verbunden. Ein ROM, in dem überwiegend Anwendersoftware enthalten ist und ein Test-ROM sind über ein Schaltmittel MUX, das ein Multiplexer sein kann, ebenfalls mit dem Bus verbunden. Das Schaltmittel MUX ist beispielsweise über das Eingangs/ Ausgangstor I/O gesteuert durch die CPU ansteuerbar, was durch einen Pfeil St angedeutet ist.

In erfindungsgemäßer Weise kann über das Schaltmittel MUX immer nur entweder das ROM oder das Test-ROM mit dem Bus verbunden und adressiert werden. Die Adressen, mit denen das ROM adressiert werden kann, sind zumindest teilweise identisch mit den Adressen, mit denen das Test-ROM adressiert werden kann. Es ist daher anhand der Adressen nicht zu erkennen, ob das ROM oder das Test-ROM adressiert ist.

Der Bus ist über das Schaltmittel MUX irreversibel mit dem ROM verbindbar, so daß nach Ablauf der Testphase das Test-ROM vollständig vom Bus abgetrennt werden kann.

Im Test-ROM ist vorzugsweise lediglich ein für den Start eines Tests erforderliches Testbeginnprogramm abgespeichert. Dieses wird nach einem Power-on-Reset aufgerufen, so daß Testroutinen von außerhalb in das X-RAM geladen und von dort ausgeführt werden können. Das Schreiben der Testroutinen in das X-RAM hat den Vorteil, daß dieser Vorgang einerseits wesentlich schneller abläuft und andererseits nur flüchtig ist, so daß die im X-RAM stehenden Testroutinen beispielsweise durch Abschalten der Versorgungsspannung schnell wieder gelöscht werden können. Nach Abschluß des Tests wird das Schaltmittel MUX irreversibel in einen Zustand gebracht, der einen Zugriff auf das Test-ROM über den Bus unmöglich macht.

Fig. 2 zeigt etwas detaillierter eine vorteilhafte Weiterbildung der erfindungsgemäßen integrierten Schaltung. Das Eingangs/Ausgangstor I/O ist wie bereits erwähnt über einen Adreßdekoder mittels einer SFR (Special Function Register)-Adresse über den Bus von der CPU adressierbar, die ihrerseits parallele Verbindungen zum Bus hat. Wenn das Eingangs/ Ausgangstor I/O über die SFR-Adresse angesteuert wird, werden die ein- und ausgehenden Daten über den Bus zur bzw. von der CPU transportiert. In der CPU kann programmgesteuert mittels des Akkumulators eine Serien/ Parallel- beziehungsweise Parallel/Serienwandlung ein- beziehungsweise ausgehender Daten stattfinden.

In erfindungsgemäßer Weise ist parallel zu diesem Übertragungspfad ein Schieberegister SR geschaltet, mittels dem eine schnelle Serien/Parallel- beziehungsweise Parallel/Serien-Wandlung während der Testphase erfolgen kann. Das Schieberegister SR wird von der CPU ebenfalls über eine SFR-Adresse angesprochen und gelesen. Hierzu ist ein entsprechender Adreßdecoder SFR beim Schieberegister SR vorgesehen. Über diese SFR-Adresse ist das Schieberegister von der CPU auch aktivier- und deaktivierbar.

Damit erkannt werden kann, wann ein zu wandelndes Wort in das Schieberegister SR eingeschrieben ist, ist ein Zähler Z vorgesehen, der die Takte Cl, mit dem die Information in das Schieberegister SR eingeschrieben werden, zählt und jeweils nach einem Wort ein Signal an die CPU abgibt, die das Einschreiben in das X-RAM steuert.

Da eine CPU in integrierten Schaltungen üblicherweise 8Bit parallel verarbeiten kann, genügt im Prinzip ein 8Bit langes Schieberegister. Zur Synchronisation des Datenstromes muß dann ein einzelnes Startbit ausreichen. Nach jeweils 8 vom Zähler Z gezählten Takten findet dann eine Serien/Parallel-Wandlung beim Einlesen statt, indem der Inhalt des Schieberegisters SR parallel auf den Bus gegeben wird.

Es ist aber auch möglich, vor jedem einzulesenden Byte ein Startbit zu senden, wodurch die Verwendung eines Personal Computers als Tester vereinfacht würde. Dann ist aber ein 9Bit langes Schieberegister nötig. Außerdem wäre die Datenübertragungsrate geringer.

Die Erfindung läßt sich prinzipiell bei jeder beliebigen von einer CPU verarbeitbaren Wortbreite anwenden also insbesondere auch bei 16Bit- und 32Bit-Zentraleinheiten. Das Schieberegister muß dann lediglich eine entsprechende Länge haben.

Ein möglicher Ablauf eines Tests läuft wie folgt ab: Zunächst sendet der Tester eine logische "0", um den Beginn eines Datentransfers anzuzeigen. Damit wird der Zähler Z freigegeben, der nach jeweils 8 Takten anzeigt, daß ein Byte abzuholen ist. Die CPU kann dies durch ein spezielles Signal erfahren, es ist aber genau so gut möglich, diesen Zeitraum durch eine Software einzustellen. In der Warteschleife, in der die CPU auf den Beginn einer Übertragung wartete, wurde vorher der Adreßzähler des X-RAMs auf seinen Anfang eingestellt. Nach der Übertragung wird nun zunächst die Testroutine aufgerufen, anschließend springt die CPU wieder in die Empfangs-Warteschleife.

In der Pause zwischen zwei Übertragungen ist es möglich, den Zähler Z weiterlaufen zu lassen. Dadurch können interne Signale 8 Takte lang mit dem Systemtakt Cl mit dem Inhalt des Schieberegisters SR über eine beliebige Funktion wie zum Beispiel ein XOR verknüpft werden (Sammelphase) und in den nächsten 8 Takten ausgegeben werden (Ausgabephase). Die Verknüpfung ist durch einen Doppelpfeil vom Schieberegister SR zum XOR-Gatter angedeutet. Tatsächlich wird das Ausgangssignal des Schieberegisters SR über das XOR auf seinen Eingang rückgekoppelt werden. Das XOR kann zum Zwecke der Verschlüsselung gesteuert von der CPU ein- bzw. ausgeschaltet werden. Dies ist durch einen Pfeil Pf angedeutet. In jeder Sammelphase kann dieser Vorgang durch ein Startbit unterbrochen werden, so daß ein neuer Datenstrom empfangen werden kann. Die Verknüpfung der internen Signale mit dem Inhalt des Schieberegisters SR während der Sammelphase hat zwei Gründe. Zum einen können dadurch alle 8 Werte, die in der Sammelphase verknüpft werden, auf ihre Korrektheit geprüft werden; zum anderen wird dadurch kein Originalsignal an die Außenwelt weitergegeben, so daß ein Mißbrauch dieser Information für potentielle Angreifer nicht möglich ist.

Diese vorteilhafte Weiterbildung dient der Erhöhung der Testabdeckung und der früheren Erkennung von defekten Chips, sofern die Defekte an den beobachteten internen Signalen erkennbar sind.

Patentansprüche

1. Integrierte Schaltung mit einer CPU, einem Anwender-ROM sowie einem diese verbindenden Bus, **gekennzeichnet durch** ein ebenfalls mit dem Bus verbundenes Test-ROM, dessen Adressraum innerhalb des Anwender-ROM-Adressraums liegt, ein mit dem Bus verbundenes, CPU-externes RAM (XRAM) sowie ein Schaltmittel (MUX), das einen Zugriff nur entweder auf das Anwender-ROM oder das Test-ROM ermöglicht.

2. Integrierte Schaltung mit einer CPU, einem Anwender-ROM sowie einem diese verbindenden Bus, auf die ein Zugriff nur über zumindest ein serielles Eingangs-/Ausgangstor (I/O) möglich ist und eine interne Serien/ Parallel-Wandlung einkommender bzw. Parallel/Serienwandlung ausgehender Daten Programmgesteuert durch die CPU erfolgt, gekennzeichnet durch ein ebenfalls mit dem Bus verbundenes Test-ROM, dessen Adressraum innerhalb des Anwender-ROM-Adress-

raums liegt, ein CPU-externes RAM (XRAM) sowie ein Schaltmittel (MUX), das einen Zugriff nur entweder auf das Anwender-ROM oder das Test-ROM ermöglicht.

3. Integrierte Schaltung nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß das Schaltmittel (MUX) irreversibel in einen Zustand bringbar ist, der nur einen Zugriff auf das Anwender-ROM erlaubt.

4. Integrierte Schaltung nach Anspruch 2 oder 3, dadurch gekennzeichnet, daß das serielle Eingangs-/Ausgangstor (I/O) zur Serien/Parallel-Wandlung zusätzlich über ein aktivier- und deaktivierbares Schieberegister (SR) mit einem internen Bus verbindbar ist.

5. Integrierte Schaltung nach Anspruch 4, dadurch gekennzeichnet, daß die Deaktivierung des Schieberegisters (SR) irreversibel durchführbar ist.

6. Integrierte Schaltung nach Anspruch 4, dadurch gekennzeichnet, daß das Schieberegister (SR) über ein logisches Gatter (XOR) rückgekoppelt ist.

7. Verfahren zum Testen einer integrierten Schaltung, die eine CPU und ein Test-ROM sowie ein CPU-externes RAM aufweist, mit den Schritten:

- nach einem Power-On-Reset wird ein im Test-ROM implementiertes Testbeginnprogramm aktiviert,
- gesteuert durch das Testbeginnprogramm werden Testroutinen in das RAM geladen und von dort durch die CPU ausgeführt,
- nach dem Ende des Tests werden die Testroutinen im RAM gelöscht und ein Ausführen des im Test-ROM implementierten Testbeginnprogramms irreversibel unterbunden.

8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, daß die Testroutinen über ein serielles Eingangs-/Ausgangstor (I/O) und einen zuschaltbaren Serien/Parallel-Wandler in das RAM geschrieben werden.

Hierzu 1 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 197 11 478 A1
Int. Cl.[6]: G 06 F 12/14
Offenlegungstag: 1. Oktober 1998

FIG 1

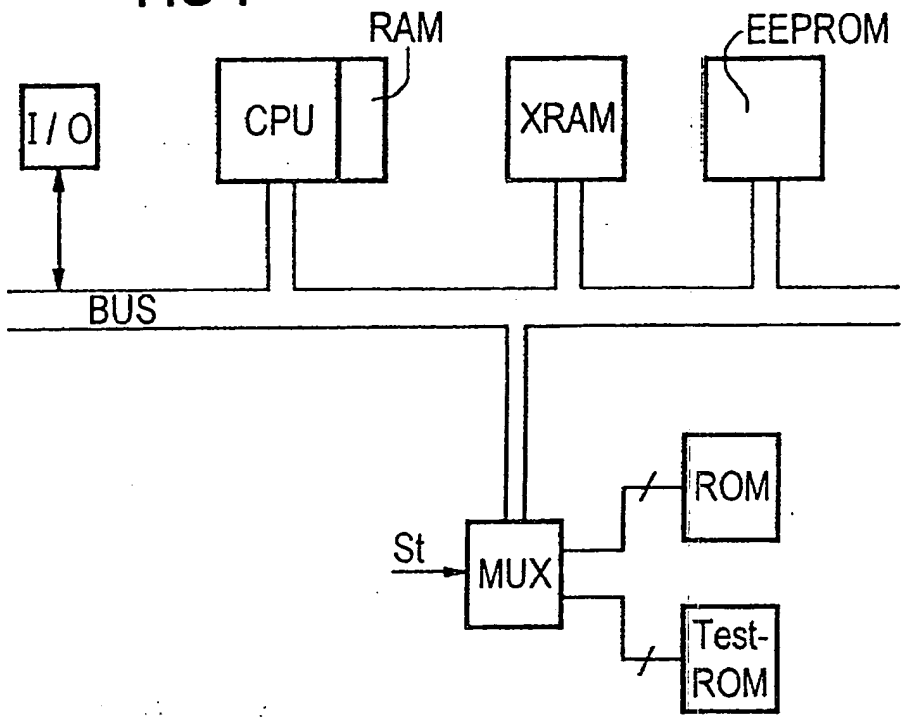


FIG 2